

## SHORT GUIDE TO STANDARDS-BASED INTERCEPTION

### Challenges of Lawful Interception to Law Enforcement Agencies (LEAs):

- Targets use many different types of services: fixed line telephone, mobile telephone, Internet (email, Voice-over-IP, Web, Instant Messaging, streaming, etc.)
- The services are constantly evolving, with new services gaining fast acceptance by criminals and terrorists.
- LEAs must interact with many different network operators; i.e., different companies providing telephone, mobile, Internet access, email, etc.
- The network operators must support a diversity of network equipment vendors and constantly evolving services. This drives up costs for interception.

### Result:

- Lawful interception becomes very complicated for the LEA (and network operator).
- LEAs must adapt separate interception practices for handling each service type and each network operator.
- Wasted time, effort and money in equipping LEA to handle multiple services and carriers.
- Fewer interceptions conducted because of excessive resources required ⇒ increased risk of criminality and terrorism.



### How can the LEA conduct fast, easy, and compliant lawful surveillance of targets despite the above challenges?

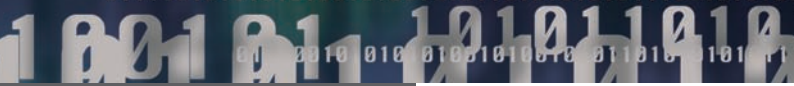
#### Solution: LEAs should have a common interface to all network operators that supports:

- Acquisition of intercepted calls and data – regardless of what services the target uses and what network operator supplies the services.
- Compatibility and easy integration through standards with any monitoring facility at the LEAs.
- Easy-to-use interface for the network operator and simple administration.

### Standards-based interception practices provide the solution.

They divide the functions of interception into 3 parts:

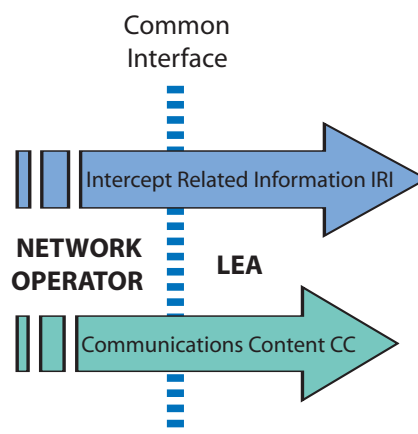
- 1. Administration.** This is the set up of the interception session, as specified by the identity of the target to be intercepted, when the interception is to take place, and what information is to be collected. Target identities can be the target's telephone number (for fixed line or mobile interception), the hardware equipment address of their modem (as in DSL and cable modem interception), or the IP address assigned to the target during dial-up Internet access.
- 2. Delivery of Interception Related Information (IRI).** This is information that describes target events during interception *as they occur*. These events can include when the target places a call and hangs up, who the target talks to (as identified by the destination's telephone number), when the target connects to the internet, who the target sends email to, from whom an instant message is received, etc.
- 3. Content of Communication (CC)** is the actual telephone conversation, fax, email, etc. that is sent from or received by the target. This content must be replicated by the network operator, and delivered to the LEA *in real time* via a systematic manner, regardless of the underlying type of data (namely voice, fax, email, web session, etc.)



## Interception Data Transfer from Network Operator to LEA

**Telephone:** Number Dialed, Calling party number, time  
**Mobile:** SIM card ID, mobile phone ID, location (future)  
**Email:** "To", "From", "cc", "Date"  
**Web:** web site visited (URL) and when

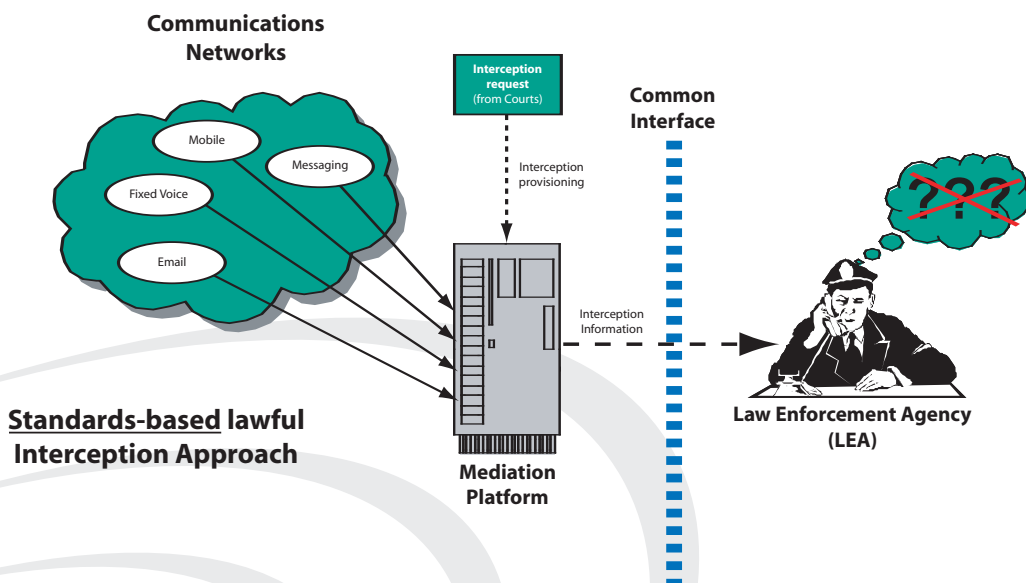
**Telephone:** real time capture of voice conversation  
**Mobile:** real time capture of voice conversation  
**Email:** email message  
**Web:** web site contents



## But how does the LEA (and network operator) handle the diversity of services and network equipment?

**Answer:** The Standards-based Mediation Platform

The Mediation Platform "bridges" the diverse forms of interception administration and collection from different services, different data types (e.g., packet IP vs. TDM), and different vendors of network equipment (Ericsson, Alcatel, Nokia, Cisco, Lucent, etc.)



### The Result:

- One user command interface at the network operator for controlling interception of all services.
- One form of delivery of intercepted traffic to the LEA.
- Very Secure Solution – closed to outside world, with authentication, confidentiality, integrity, and comprehensive logging of all system actions.
- Administered by only specially trained and screened personnel.

When the network operator acquires IRI and CC, the target must never know they are being intercepted! All interception and delivery functions must be carefully engineered to ensure transparency of the interception from the target's perspective. Mediation helps to assure this requirement.

*Everybody's job is now easier and much less costly!*

AQSACOM develops and markets real time Lawful Interception, Mobility Tracking and Surveillance solutions. With its core business focused on lawful interception and related applications for over eleven years, AQSACOM provides end-to-end turnkey solutions for fulfilling lawful interception requirements anywhere in the world, especially over highly heterogeneous networking and services environments. AQSACOM's diversified customer portfolio includes clients from more than 30 countries, covering geographical areas as diverse as Central and Eastern Europe, Asia-Pacific, North America, Africa and the Middle-East.



[www.aqsacom.com](http://www.aqsacom.com)

AQSACOM Americas  
 Washington, DC  
 Tel: +1 202 315 3943

AQSACOM Europe  
 Paris  
 Tel: +33 1 6929 8400

email: [sales@aqsa.com](mailto:sales@aqsa.com)

AQSACOM Asia  
 Melbourne, Australia  
 Tel: +61 3 9909 72 80

